

Amendments to the Claims

This listing of claims will replace all prior versions, and listings, of claims in the application.

1-9. (Canceled)

10. (Currently amended) A method for providing access to a secured document, the method comprising:

requesting authentication of ~~authenticating~~ a user having credential information to a first server at a first location having a first instance of the secured document stored therein;

in response to determining that the user is authenticated to the first server,
requesting that a connection be established that allows the user to access the first
instance of the secured document at the first server; and

upon receiving a request from the user to ~~[[for]]~~ access a second instance
of ~~[[to]]~~ the secured document at a second server at a second location~~[[,]]~~:

requesting authentication of ~~authenticating~~ the user credential
~~information to the second server~~~~[[, and]]~~;

determining whether access to the secured document is permitted
from the second location via the second server;

in response to determining that the user is authenticated to the
second server and that access to the secured document is permitted from
the second location, requesting disconnection of ~~disconnecting~~ the user
from the first server; and

~~before establishing~~ requesting that a connection be established that allows the user to access ~~[[to]]~~ the second instance of the secured document at the second server.

11. (Currently amended) The method as recited in claim 10, wherein the requesting authentication of ~~authenticating~~ a user having credential information comprises authenticating both the credential information and a client machine at the first location.

12. (Currently amended) The method as recited in claim 10, further comprising enabling the user to use ~~wherein~~ the first and the second servers ~~[[are]]~~ as access points to gain access to the secured document.

13. (Currently amended) The method as recited in claim ~~[[29]]~~ 12, wherein:
in response to receiving a request from the user for access to the first instance of the secured document at the first location, causing the first server to interact ~~interacts~~ over a network with the user, and

in response to receiving ~~[[a]]~~ the request from the user for access to the second instance of the secured document at the second location, causing the second server to interact ~~interacts~~ over a network with the user using a second client machine at the second location.

14. (Cancelled)

15. (Previously presented) The method as recited in claim 29, wherein the authenticating the credential information to the first server occurs in response to receiving a request for access to the secured document at the first location, and wherein the receiving the request for access via the second server occurs in response to receiving a request a request for access to the secured document at the second location.

16. (Previously presented) The method as recited in claim 17, wherein the authenticating the credential information to the second server further comprises:

upon receiving the request for access to access the secured document via the second server, determining permitted locations from which the secured document is permitted to be accessed from;

determining whether the second location is one of the permitted locations;

and

bypassing the disconnecting the user from the first server in response to the determining that the second location is not one of the permitted locations.

17. (Currently amended) The method as recited in claim 30, wherein:

in response to receiving [[a]] the request from the user for access to the secured document at the first location, the first server interacts over a network with the user using a first client machine at the first location, and

in response to receiving [[a]] the request from the user for access to the secured document at the second location, the second server interacts over a network with the user using a second client machine at the second location.

18. (Currently amended) An article of manufacture including a computer-readable medium having instructions stored thereon, that, in response to execution if executed by a computing device, cause the computing device to perform operations comprising:

requesting authentication of authenticating a user having credential information [[to]] at a first server having a first instance of a secured document stored therein;

in response to determining that the user is authenticated to the first server,
requesting that a connection be established that allows the user to access the first
instance of the secured document at the first server; and

upon receiving a request from the user to [[for]] access a second instance
of [[to]] the secured document at a second server from a second location~~[[,]]~~;

requesting authentication of authenticating the user credential
information to the second server~~[[, and]]~~;

determining whether access to the second instance of the secured
document is permitted from the second location via the second server;

in response to determining that the user is authenticated to the
second server and that access to the secured document is permitted from
the second location, requesting disconnection of disconnecting the user
from the first server; and

~~before establishing~~ requesting that a connection be established that
allows the user to access [[to]] the second instance of the secured
document at the second server.

19. (Currently amended) The article of manufacture as recited in claim
[[31]]18, wherein:

in response to receiving [[a]] the request from the user for access to the
secured document at the first location, causing the first server to interact ~~interacts~~
over a network with the user, and

in response to receiving [[a]] the request from the user for access to the
secured document at the second location, causing the second server to interact
~~interacts~~ over a network with the user using a second client machine at the second
location.

20. (Previously presented) The article of manufacture as recited in claim 32,
the operations further comprising:

determining, prior to the reconfiguring of either the first local module at
the first server or the second local module at the second server, whether the user
having the credential information is permitted to access the secured document
from the second location via the second server.

21. (Currently amended) A system for controlling access to a secured
document, comprising:

an access control device configured to:

request authentication of ~~authenticate~~ a user having credential
information by [[to]] a first server having a first instance of the secured
document stored therein;

in response to determining that the user is authenticated by the first server, request that a connection be established that allows the user to access the first instance of the secured document at the first server; and
upon receiving a request from the user for access to a second instance of the secured document stored at a second server ~~from a second location: [[,]]~~

request authentication of ~~authenticate the user by credential information to the second server~~ [[, and]];

determine whether the second server permits access to the second instance of the secured document;

in response to determining that the user is authenticated to the second server and that the second server permits access to the second instance of the secured document, request that ~~disconnect the user be~~ disconnected from the first server; and

~~before establishing~~ request that a connection be established that allows the user to access [[to]] the secured document at the second server.

22. (Previously presented) The article of manufacture as recited in claim 31, wherein authenticating the credential information comprises authenticating both the credential information and a client machine.

23. (Previously presented) The article of manufacture as recited in claim 32, the operations further comprising:

determining, prior to the reconfiguring the first local module at the first server and the second local module at the second server, whether the user having the credential information is permitted to access to the secured document from the second location via the second server.

24. (Previously presented) The article of manufacture as recited in claim 33, wherein the authenticating the credential information to the second server further comprises:

upon receiving the request for access to the secured document via the second server, determining permitted locations from which the secured document is permitted to be accessed from;

determining whether the second location is one of the permitted locations;
and

bypassing the disconnecting the user from the first server in response to the determination that the second location is not one of the permitted locations.

25. (Previously presented) The system as recited in claim 21, wherein the access control device is further configured to authenticate both the credential information and a client machine.

26. (Previously presented) The system as recited in claim 21, wherein the first and the second servers are access points to gain access to the secured document.

27. (Previously presented) The system as recited in claim 35, wherein the access control device is further configured to determine, prior to reconfiguring the first local module at the first server and the second local module at the second server, whether access to the secured document is permitted from the second location via the second server.

28. (Canceled)

29. (Previously presented) The method as recited in claim 10, further comprising:

authenticating the credential information to the first server with respect to a previous request for access;
subsequently receiving the request for access via the second server; and
authenticating the credential information to the second server with respect to the request for access.

30. (Previously presented) The method as recited in claim 29, wherein the disconnecting the user from the first server comprises:

upon receiving the request for access via the second server, identifying a first local module previously supporting a connection from the first server;
reconfiguring the first local module at the first server to remove support for access to the secured document at the first server;
identifying a second local module to support access to the secured document at the second server; and

reconfiguring the second local module at the second server to add support for access to the secured document at the second server.

31. (Currently amended) The article of manufacture as recited in claim 18, the operations further comprising:

authenticating the credential information to the first server with respect to a previous request for access;

subsequently receiving the request for access via the second server; and

authenticating the [[the]] credential information to the second server with respect to the request for access.

32. (Previously presented) The article of manufacture as recited in claim 31, wherein the disconnecting the user from the first server comprises:

upon receiving the request for access via the second server, identifying a first local module previously supporting access to the secured document at the first server;

reconfiguring the first local module at the first server to remove support for access to the secured document at the first server;

identifying a second local module to support access to the secured document at the second server; and

reconfiguring the second local module at the second server to add support for access to the secured document at the second server.

33. (Previously presented) The article of manufacture as recited in claim 32, wherein:

in response to receiving a request for access to the secured document at the first location, the first server interacts over a network with the user using a first client machine at the first location, and

in response to receiving a request for access to the secured document at the second location, the second server interacts over a network with the user server using a second client machine at the second location.

34. (Previously presented) The system as recited in claim 21, wherein the access control device is further configured to:

authenticate the credential information to the first server with respect to a previous request for access;

subsequently receive the request for access via the second server; and

authenticate the credential information to the second server with respect to the request for access.

35. (Previously presented) The system as recited in claim 34, wherein the access control device is further configured to:

identify a first local module previously supporting the client machine at the first server upon receiving the request for access to the secured document via the second server;

reconfigure the first local module at the first server to remove support for access to the secured document at the first server;

identify a second local module to support access to the secured document
at the second server; and
reconfigure the second local module at the second server to add support
for access to the secured document at the second server.